PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:
H04L 9/08	A1	WO 00/42731
		(43) Date de publication internationale: 20 juillet 2000 (20.07.00)

(21) Numéro de la demande internationale: PCT/FR00/00099

(22) Date de dépôt international: 18 janvier 2000 (18.01.00)

(30) Données relatives à la priorité:
99/00462 18 janvier 1999 (18.01.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F–92120 Montrouge (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: • BUTNARU, Dan [FR/FR]; 61, rue des Longaines, F–91330 Yerres (FR). •GELZE, Mathias [FR/FR]; 15, rue Poirier de Narçay, F–75014 Paris (FR).•ROSSET, Raphaël [FR/FR]; 4, place du 11 Novembre, F–78220 Viroflay (FR).

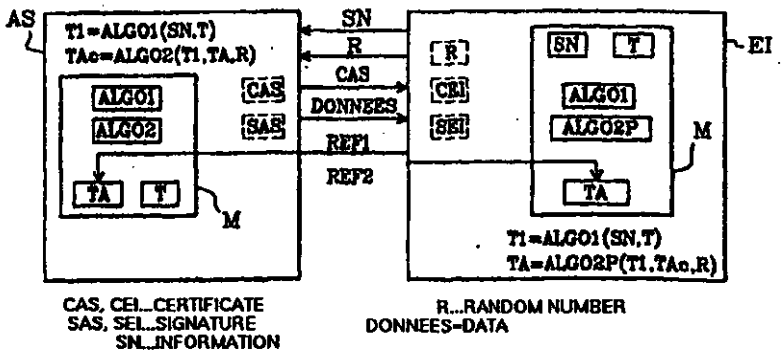
(74) Mandataire: UTZMANN–NORTH, Anne; Schlumberger Systèmes Test & Transactions, 50, avenue Jean Jaurès, Boîte postale 620–12, F–92542 Montrouge Cedex (FR).

(81) Etats désignés: CN, MX, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR SECURE DATA LOADING BETWEEN TWO SECURITY MODULES

(54) Titre: PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE



(57) Abstract

The invention concerns a method for customizing a security module comprising a secure loading of an application key from a first security module to a set of second security modules, said first and second security modules comprising each at least a storage unit. The invention is characterised in that said method comprises steps which consist, at each loading, in: calculating in the first and second modules an operating key from a transport key identical for each second module of said set; using the operating key for encrypting the application key in the first module; then sending the application key to the second module, decrypted and verified in said module. The operating key is not recorded in the storage unit of the security modules. The invention is particularly applicable in the field of banking.

(57) Abrégé

L'invention concerne un procédé de personnalisation de module de sécurité comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers un ensemble de plusieurs deuxièmes modules de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire. L'invention se caractérise en ce que ledit procédé comporte des étapes selon lesquelles, lors de chaque chargement, on calcule dans le premier et deuxièmes modules une clef d'exploitation à partir d'une clef de transport identique pour chaque deuxième module dudit ensemble. La clef d'exploitation est utilisée pour le chiffrement dans le premier module de la clef applicative. Cette dernière est par la suite envoyée au deuxième module, déchiffrée et vérifiée dans ledit module. La clef d'exploitation n'est pas enregistrée dans la mémoire des modules de sécurité. L'invention s'applique, en particulier au domaine bancaire.

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

La présente invention concerne un procédé de personnalisation d'un ensemble de plusieurs deuxièmes modules de sécurité, comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers lesdits deuxièmes modules de sécurité dudit ensemble, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire.

L'invention trouve une application particulièrement avantageuse lors d'une phase de personnalisation de deuxièmes modules de sécurité dans les domaines tels que le domaine de la fidélité ou le domaine bancaire.

Un tel procédé de personnalisation est effectué avant une phase d'utilisation desdits deuxièmes modules. Par exemple, lors d'une phase d'utilisation dans le domaine de la fidélité, les deuxièmes modules se trouvent dans des terminaux de stations service et sont utilisés de manière à fournir des prestations de sécurisation de transactions de débit-crédit de points de fidélité entre un desdits terminaux et des cartes de crédit d'utilisateurs. Dans le domaine bancaire, les deuxièmes modules se trouvent dans des terminaux bancaires et fournissent des prestations de sécurisation de transactions d'argent dans des cartes de crédit d'utilisateurs.

Un état de la technique connu et divulgué dans le brevet américain publié sous le numéro US 5 517 567 au nom de DAQ Electronics enseigne qu'il existe un système de cryptage de clef dont le but est une sécurisation des communications pouvant s'établir entre un deuxième module de sécurité « master unit» et un troisième module utilisateur « remote unit » lorsque ce dernier est installé dans un site distant, par exemple dans un téléphone portable. Ladite sécurisation est basée sur l'utilisation d'une clef de communication temporaire.

Selon ce système, après que le module utilisateur est installé sur son site distant, on génère au moyen du deuxième module une clef de communication. Par suite, on envoie pour l'établissement de chaque communication, à partir du deuxième module au module utilisateur, la clef de communication chiffrée. La clef de communication permet un échange de messages sécurisés entre le deuxième module et le module utilisateur car elle n'est connue que de ces deux modules. En effet, ladite clef est basée sur une paire de deux nombres secrets unique à chaque module utilisateur et le deuxième module comporte toutes les paires correspondant à tous les modules utilisateurs. Le système est d'autant plus sécurisé qu'une paire de deux nombres secrets est inscrite dans la mémoire d'un module utilisateur, ladite mémoire étant volatile. Ainsi, lorsqu'une communication est terminée et lorsque le module utilisateur n'est plus alimenté, ladite paire est effacée et un fraudeur ne risque pas de découvrir les deux nombres secrets. Pour établir une autre communication, ledit système génère une autre clef de communication.

Le document cité ci-dessus décrit un système mis en oeuvre lors d'une phase d'utilisation d'un deuxième module et d'un module utilisateur, dont le but est d'établir une communication sécurisée entre les deux modules en utilisant une même clef de communication dédiée à une communication. Il ne décrit en aucune façon un système de personnalisation dont le but serait de sécuriser un chargement de clef dans un ensemble de plusieurs deuxièmes modules de sécurité.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de personnalisation d'un ensemble de plusieurs deuxièmes modules de sécurité comprenant un chargement sécurisé d'une clef applicative à partir d'un premier module de sécurité vers lesdits deuxièmes modules de sécurité dudit ensemble, lesdits premier et deuxièmes modules comprenant chacun au moins

une mémoire, qui permettrait, d'une part, d'éviter à un fraudeur de découvrir ladite clef applicative, et, d'autre part, de gagner du temps lors de la phase de personnalisation desdits deuxièmes modules de sécurité.

Une solution au problème technique posé se caractérise en ce que ledit procédé de personnalisation comporte les étapes selon lesquelles :

pour chaque deuxième module dudit ensemble,

- lors de chaque chargement, on calcule dans le premier module une clef d'exploitation à partir d'une information propre au deuxième module, d'une clef de transport et d'un algorithme de diversification, ladite clef de transport se trouvant dans la mémoire du premier module de sécurité, ladite mémoire étant non volatile,
- on chiffre dans le premier module la clef applicative, à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de cryptage, ladite clef applicative se trouvant dans ladite mémoire,
- on envoie au deuxième module des données comprenant la clef applicative chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module la clef d'exploitation à partir de l'information propre au deuxième module, de la clef de transport et de l'algorithme de diversification, ladite même clef de transport se trouvant dans la mémoire non volatile de chaque deuxième module de sécurité dudit ensemble, ladite clef d'exploitation n'étant pas enregistrée dans la mémoire dudit deuxième module,
- on déchiffre dans le deuxième module la clef applicative chiffrée, à partir d'informations comprenant ladite clef d'exploitation et d'un algorithme de décryptage inverse de l'algorithme de cryptage.

Ainsi, comme on le verra en détail plus loin, le procédé de chargement de l'invention permet, en calculant ladite clef d'exploitation et en ne la conservant que le temps du chiffrement ou du déchiffrement de la clef applicative, d'améliorer la sécurité du chargement d'une clef applicative. Par suite, un fraudeur ne pourra accéder à ladite clef d'exploitation ni par conséquent à la clef applicative. Les éventuelles fraudes sont par conséquent évitées et on n'effectue plus d'opérations qui sont coûteuses en temps pour la phase de personnalisation, le temps de calcul de la clef d'exploitation étant infime par rapport au temps d'accès nécessaire à l'enregistrement de ladite clef.

La description qui va suivre au regard des dessins annexés, donnée à titre d'exemple non limitatif, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant un premier module et plusieurs deuxièmes modules appartenant à un même ensemble.

La figure 2 est un schéma montrant le premier module et un deuxième module de la figure 1.

La figure 3 est un schéma montrant un échange de données entre le premier module et le deuxième module de la figure 2.

La figure 4 un schéma montrant un deuxième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 5 est un schéma montrant un troisième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 6 est un schéma montrant un quatrième échange de données entre le premier module et le deuxième module de la figure 2.

Sur la figure 1 est représenté un premier module AS de sécurité et plusieurs modules EI de sécurité d'un même ensemble S (non représenté), chacun des modules (AS,EI) comprenant au moins une mémoire M non volatile. Le premier module AS ainsi que les deuxièmes modules EI dudit ensemble S comportent une même clef T de transport

et un même algorithme ALGO1 appelé algorithme de diversification qui se trouvent dans la mémoire M. Sur la figure 2, sont représentés le module AS ainsi qu'un module EI dudit ensemble S. Chaque deuxième module EI de l'ensemble S comporte la même clef de transport T. Ainsi, on différencie un ensemble de deuxièmes modules EI d'un autre ensemble au moyen de ladite clef de transport T. Par exemple, deux ensembles de deuxièmes modules EI correspondent à deux fournisseurs de stations service différents.

En outre, le premier module AS comporte une clef applicative TA et un algorithme ALGO2 de cryptage. On notera que les deux algorithmes ALGO1 et ALGO2 peuvent utiliser un même algorithme de base. Chaque module EI dudit ensemble S comprend une information SN qui lui est propre et au moins une application utilisateur (non représenté), par exemple une application fournissant des prestations de sécurisations de transactions de débit-crédit de points de fidélité.

Afin d'utiliser les modules EI de sécurité dudit ensemble S, il faut pour chaque deuxième module EI dudit ensemble S, au préalable charger une clef applicative TA du premier module AS lors d'une phase dite de personnalisation comprenant les étapes décrites ci-après. Ladite clef est transférée par l'intermédiaire d'un réseau de communication standard. On empêche un fraudeur qui espionnerait ledit réseau ou lesdits modules d'accéder à des clefs des modules, comme décrit ci-après.

Dans une première étape, lors de chaque chargement, on calcule dans le premier module AS une clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite clef T de transport se trouvant dans la mémoire M du premier module AS de sécurité, ladite mémoire étant non volatile. Préférentiellement, ladite mémoire M est une mémoire réinscriptible. On notera que la clef de

transport T demeure valide même pendant les phases d'utilisation d'un deuxième module EI, tant qu'on ne la remplace pas.

L'information SN propre au deuxième module EI ne se trouve pas dans le premier module. Aussi, comme le montre la figure 3, on envoie au premier module AS l'information SN propre au deuxième module EI, préalablement au calcul dans le premier module AS de la clef T1 d'exploitation. Ledit premier module AS comporte préférentiellement plusieurs clefs applicatives TA. Ladite clef T1 va servir au chargement d'une des clefs applicatives TA contenues dans le premier module AS, ladite clef applicative choisie sera chiffrée et envoyée au module EI. Une clef applicative est associée à une application utilisateur. Suivant l'application se trouvant dans le deuxième module EI, on choisit la clef adéquate.

Comme le montre la figure 3, pour choisir une desdites clefs applicatives TA, dans une deuxième étape, on envoie au premier module AS une information REF1 relative à une clef applicative TA, préalablement au chiffrement dans ledit module AS de la clef applicative TA et on choisit la clef applicative TA à chiffrer à partir de ladite information REF1. On peut par exemple envoyer à partir du deuxième module EI une référence représentant un numéro de clef ayant une valeur de trois pour indiquer que l'on choisit la troisième clef correspondant à une application dudit module EI. C'est cette dernière qui sera chargée dans le deuxième module EI. S'il n'existe pas de clef applicative TA référencée par ledit nombre REF1, le premier module AS indique que ladite clef n'existe pas.

Dans une troisième étape, comme le montre la figure 3, on chiffre dans le premier module AS la clef applicative TA à partir d'informations comprenant ladite clef T1 d'exploitation et de l'algorithme ALGO2 de cryptage. Ladite clef d'exploitation se trouve temporairement dans une deuxième mémoire volatile (non représentée) du premier module AS.

Afin de protéger le premier module AS contre une éventuelle fraude, postérieurement au chiffrement de la clef applicative TA, on efface la clef T1 d'exploitation sauvegardée temporairement dans ladite deuxième mémoire volatile du premier module AS.

Après avoir chiffré ladite clef TA, on envoie au deuxième module EI des données DONNEES comprenant la clef applicative TA chiffrée.

Dans une quatrième étape, on déchiffre dans le deuxième module EI la clef applicative TA chiffrée, à partir d'informations comprenant ladite clef T1 d'exploitation et d'un algorithme ALGO2P de décryptage inverse de l'algorithme ALGO2 de cryptage. Dans cette étape, afin de retrouver la clef applicative TA choisie, il est nécessaire d'utiliser la même clef T1 d'exploitation qui a été utilisée pour le cryptage de ladite clef applicative TA dans le premier module AS de sécurité. A cette fin, préalablement au déchiffrement de la clef applicative TA chiffrée, lors de chaque chargement, on calcule dans le deuxième module EI la clef T1 d'exploitation à partir de l'information SN propre au deuxième module EI, de la clef T de transport et de l'algorithme ALGO1 de diversification, ladite même clef T de transport se trouvant dans la mémoire M non volatile de chaque deuxième module EI de sécurité dudit ensemble S, ladite clef T1 d'exploitation n'étant pas enregistrée dans la mémoire M d'un deuxième module EI. Préférentiellement la mémoire M du deuxième module est réinscriptible. Ladite clef T1 d'exploitation est sauvegardée temporairement dans une deuxième mémoire volatile (non représentée) du deuxième module EI.

On notera que ledit calcul peut se faire à tout moment avant le déchiffrement de la clef applicative TA. Les éléments nécessaires au calcul de la clef T1 d'exploitation dans le deuxième module EI de sécurité sont les mêmes que ceux utilisés pour le calcul de la clef T1 d'exploitation dans le premier module AS. Par conséquent, les deux clefs T1 sont identiques et on retrouve bien dans le deuxième module EI

la clef applicative TA choisie. Il n'a pas été nécessaire d'envoyer la clef T1 d'exploitation à travers le réseau de communication.

Dans une cinquième étape, postérieurement au déchiffrement de la clef applicative TA et préférentiellement juste après ledit déchiffrement, on efface la clef T1 d'exploitation sauvegardée temporairement dans ladite deuxième mémoire volatile du deuxième module EI.

Le fait, d'une part, de ne pas envoyer une clef d'exploitation T1 à travers le réseau de communication, d'autre part, de ne pas enregistrer une clef T1 d'exploitation dans une mémoire M non volatile d'un deuxième module EI, et enfin, le fait que ladite clef d'exploitation n'existe dans le deuxième module que le temps de déchiffrement de la clef applicative TA, rend une fraude plus difficile à effectuer dans la mesure où si un fraudeur veut trouver une clef applicative TA, il doit auparavant retrouver la clef T1 d'exploitation utilisée. Enfin, cela facilite la personnalisation et une mise sur le terrain d'un nième deuxième module EI dans la mesure où pour personnaliser les deuxièmes modules il n'est plus nécessaire d'effectuer deux chargements, un premier d'une clef T1 d'exploitation et un deuxième d'une clef applicative TA, mais simplement un chargement d'une clef applicative TA. On se libère ainsi de du premier chargement qui est habituellement effectué par une entité différente du premier module AS, ce qui complique généralement d'autant plus les choses.

A l'instar du premier module AS, un module EI comprend préférentiellement plusieurs clefs applicatives TA. Ainsi, au moyen d'un deuxième module EI, on peut gérer plusieurs applications. De plus, cela améliore la sécurité desdits modules, étant donné qu'un fraudeur aura plus de difficulté à, d'une part, découvrir une clef applicative parmi d'autres, et d'autre part, à savoir à qu'elle application elle est dédiée. Dans l'exemple précédent concernant le domaine de la fidélité, lors de

l'utilisation d'un deuxième module EI, celui-ci doit pouvoir fournir différentes prestations telles que la sécurisation des transactions de débit-crédit de points pour par exemple différents types de carburant. Il est ainsi important d'avoir différentes clefs applicatives TA dans ledit module EI pour gérer la sécurisation de ces différents types de transactions, ces derniers représentant différentes applications.

Aussi, dans une sixième étape, on envoie au deuxième module EI une information REF2 relative à une clef applicative TA, préalablement au déchiffrement dans ledit module EI de la clef applicative TA chiffrée, comme le montre la figure 4. L'information REF2 permet, soit de choisir la clef applicative TA qui va recevoir la valeur de la clef applicative provenant du premier module AS, soit d'indiquer un emplacement où sera chargée ladite clef TA provenant dudit premier module AS. Ainsi, on peut soit modifier une valeur d'une clef TA déjà existante dans ledit deuxième module EI, soit charger une nouvelle clef applicative TA dans le deuxième module EI pour une nouvelle application utilisateur.

Dans le cas où la clef applicative TA référencée par ladite information REF2 n'existe pas ou que ledit emplacement n'existe pas ou n'est pas fait pour accueillir une clef, le deuxième module EI rejette la clef reçue et indique qu'une erreur s'est produite. On notera que les informations REF1 et REF2 envoyées respectivement au premier et deuxième modules de sécurité peuvent être équivalentes.

Par la suite, lors d'une phase d'utilisation, une des clefs applicatives TA se trouvant dans le deuxième module EI pourra être utilisée par ledit module pour s'identifier vis-à-vis d'entités extérieures comme par exemple une carte utilisateur. Or ladite identification doit être unique. Par conséquent, ladite clef TA ne doit pas avoir de doublon. Aussi, lorsque l'on veut charger cette clef, on diversifie dans le premier module AS ladite clef applicative TA choisie, préalablement au

chiffrement de ladite clef. La diversification se fait en fonction d'une information propre à chaque deuxième module.

Enfin, dans une dernière étape, on enregistre dans le deuxième module EI, après le déchiffrement de la clef applicative TA chiffrée, ladite clef TA dans ledit module EI. L'enregistrement dans ledit deuxième module EI de la clef applicative TA se fait en fonction de l'information REF2 relative à une clef applicative TA. L'enregistrement se fait dans la mémoire M non volatile réinscriptible.

Le deuxième module EI peut maintenant être utilisé et être placé sur un site utilisateur distant tel qu'un terminal de stations service. On notera qu'aucune clef T1 d'exploitation n'a été transférée du premier module AS au deuxième module EI et n'a été enregistrée dans la mémoire M des modules de sécurité. Les opérations nécessaires à ces deux actions ne sont pas effectuées ce qui permet de gagner du temps lors de la phase de personnalisation. Ainsi, on ne mémorise pas une donnée secrète immédiatement utilisable par un algorithme ce qui empêche un fraudeur qui analyse ledit algorithme de découvrir ladite donnée. Ainsi, il est inutile pour le fraudeur d'espionner soit le réseau de communication soit les modules de sécurité afin de trouver la clef T1 d'exploitation utilisée.

Un autre avantage de l'objet de la présente invention se trouve dans le fait que l'information SN propre à chaque deuxième module EI de sécurité est unique. La clef T1 d'exploitation, qui est diversifiée c'est à dire calculée à partir de cette information, est par conséquent unique pour chaque module EI de sécurité. Par suite, la clef applicative TA chiffrée, qui est fonction de ladite clef T1 d'exploitation, n'est destinée qu'à un unique deuxième module EI destinataire ce qui renforce l'aspect sécuritaire de l'invention. Si un deuxième module EI n'a pas la même information SN que celle utilisée pour calculer la clef T1 d'exploitation dans le premier module AS et s'il reçoit ainsi une clef applicative TA qui

ne lui est pas destinée, il rejette ladite clef et indique qu'une erreur s'est produite.

D'autres aspects sécuritaires décrits ci-dessous sont couverts par l'objet de la présente invention.

L'objet de la présente invention prévoit une étape supplémentaire, montrée à la figure 4, selon laquelle on envoie au premier module AS un nombre aléatoire R issu du deuxième module EI, préalablement au chiffrement dans le premier module AS de la clef applicative TA. Les informations permettant, d'une part, de chiffrer la clef applicative TA dans le premier module AS, et, d'autre part, de déchiffrer dans le deuxième module EI la clef applicative TA chiffrée, comprennent le nombre aléatoire R issu du deuxième module EI. L'utilisation du nombre aléatoire R pour chiffrer et déchiffrer ladite clef applicative TA évite d'avoir une même valeur de chiffrement d'une clef applicative TA destinée à un deuxième module EI lorsque, par exemple, l'on charge plusieurs fois ladite clef dans ledit module. Ainsi, chaque chiffrement d'une clef applicative TA destinée à un deuxième module EI est unique. Ainsi, un fraudeur qui espionne le réseau de communication et récupère les données DONNEES lors du transfert n'obtient jamais une même valeur de chiffrement et ne peut par conséquent découvrir un secret relatif à la clef applicative TA transférée.

Cependant, lors dudit transfert, le fraudeur peut avoir effectué des opérations frauduleuses qui altèrent les données transférées. Aussi, on vérifie que les données DONNEES comprenant la clef applicative TA chiffrée sont intègres. A cette fin, comme le montre la figure 5, on calcule dans le premier module AS un certificat CAS sur lesdites données DONNEES, préalablement à l'envoi desdites données, ledit certificat étant envoyé par la suite au deuxième module EI et vérifié dans ledit deuxième module, préalablement au déchiffrement dans ledit deuxième module EI de la clef applicative TA chiffrée. Afin d'effectuer la

vérification, on calcule dans le deuxième module EI un certificat CEI en fonction des données reçues et on compare les deux certificats CAS et CEI. Si une fraude ou une erreur s'est produite lors dudit transfert, la vérification du certificat CAS est erronée, le déchiffrement de la clef applicative TA ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Ce système garantit ainsi une intégrité des données DONNEES lors de leur transfert depuis le premier module AS vers le deuxième module EI sur le réseau de communication et ce avant l'utilisation d'un deuxième module EI c'est à dire avant leur mise en circulation sur le terrain. De plus, dans le cas où la vérification serait fausse, cela évite de faire un déchiffrement inutile et par suite de perdre du temps inutilement.

De même qu'il faut garantir l'intégrité des données transférées, de même il faut garantir l'authenticité des données qui sont enregistrées dans le deuxième module EI. Ainsi, on vérifie que la clef applicative TA est authentique. A cet effet, comme le montre la figure 5, on calcule dans le premier module AS, préalablement au chiffrement de la clef applicative TA, une signature SAS de ladite clef TA, ladite signature étant envoyée par la suite au deuxième module EI et vérifiée dans ledit module. La vérification de la signature de ladite clef applicative TA se fait postérieurement au déchiffrement dans le deuxième module EI de ladite clef TA chiffrée et préalablement à l'enregistrement de ladite clef dans ledit module. Afin d'effectuer la vérification, on calcule dans le deuxième module EI une signature SEI avec la clef applicative TA déchiffrée dans ledit module EI et on compare les deux signatures SAS et SEI. Dans le cas où les deux signatures sont équivalentes, la clef applicative TA déchiffrée est authentique et est enregistrée. Dans le cas où la clef applicative TA n'est pas authentique, l'enregistrement de ladite clef ne se fait pas et le deuxième module EI indique qu'une erreur s'est produite. Le système décrit ci-dessus permet ainsi de vérifier que

l'on récupère bien la clef applicative TA choisie dans le premier module AS et non une autre clef. On notera que lorsque ladite signature SAS existe, le certificat CAS est calculé également en fonction de ladite signature SAS. Ladite signature fait partie des données DONNEES envoyées lors de la troisième étape décrite précédemment.

L'envoi de données telles qu'un certificat ou une signature à un module de sécurité fait appel à des opérations dont le temps d'accomplissement s'ajoute à celui de la phase de personnalisation. Aussi, comme le montre la figure 6, afin de réduire le nombre d'accès aux différents modules et ainsi de réduire le temps de personnalisation, on envoie l'ensemble des données dont a besoin un module de sécurité en une seule fois au moyen d'une unique commande. Le nombre R aléatoire, le nombre REF1 relatif à une clef applicative TA et le nombre SN propre au deuxième module EI sont envoyés au premier module AS au moyen d'une unique première commande EXPORTKEY. De la même façon, la clef applicative TA chiffrée, le nombre REF2 relatif à une clef applicative TA, la signature SAS ainsi que le certificat CAS s'ils existent, sont envoyés au deuxième module EI au moyen d'une unique deuxième commande IMPORTKEY.

L'invention s'applique plus particulièrement dans le cas où le premier module AS de sécurité est une carte à puce. La carte à puce comprend un corps de carte plastique dans lequel est incorporé un module électronique comportant une puce à circuit intégré. Ladite puce comprend couramment deux mémoires M et une troisième mémoire volatile (RAM), la première mémoire M étant réinscriptible (EEPROM) et la deuxième non réinscriptible (ROM). La première mémoire M comprend l'ensemble des clefs applicatives TA et la clef de transport T. La troisième mémoire comprend la clef T1 d'exploitation. Celle-ci ne demeure dans ladite mémoire que le temps de chiffrement ou de déchiffrement de la clef applicative dans un module de sécurité. Les

algorithmes ALGO1 de diversification et ALGO2 de cryptage peuvent se trouver dans la première ou deuxième mémoire M. Cependant, on notera qu'il n'est pas obligatoire d'avoir lesdits algorithmes dans la carte à puce. Ils peuvent se trouver dans une entité extérieure à ladite carte à puce, par exemple dans une unité centrale d'un terminal avec lequel serait connectée ladite carte à puce.

La carte à puce permet d'assurer une meilleure protection des clefs applicatives TA. Dans une carte à puce, contrairement à un terminal d'un ordinateur par exemple, lesdites clefs sont inconnues de toute entité (d'un terminal, d'un administrateur de ladite carte, d'une autre carte à puce, ...) excepté de l'entité émettrice desdites clefs. De plus, une fraude est plus difficile à réaliser sur une carte à puce que sur une unité centrale d'un terminal par exemple. Pour les mêmes raisons, le deuxième module de sécurité est une carte à puce.

On notera qu'une clef applicative TA étant dans une mémoire M non volatile, elle peut être utilisée lors de plusieurs phases d'utilisation d'un deuxième module EI, car même lorsque ce dernier n'est plus alimenté, ladite clef n'est pas effacée.

REVENDICATIONS

1 - Procédé de personnalisation d'un ensemble (S) de plusieurs deuxièmes modules de sécurité (EI) comprenant un chargement sécurisé d'une clef applicative (TA) à partir d'un premier module (AS) de sécurité d'une unité centrale vers ledit ensemble de deuxièmes modules (EI) de sécurité, lesdits premier et deuxièmes modules comprenant chacun au moins une mémoire (M), caractérisé en ce qu'il comporte les étapes selon lesquelles :

Pour chaque deuxième module (EI) dudit ensemble (S),

- lors de chaque chargement, on calcule dans le premier module (AS) une clef (T1) d'exploitation à partir d'une information propre au deuxième module (EI), d'une clef de transport (T) et d'un algorithme de diversification (ALGO1), ladite clef de transport (T) se trouvant dans la mémoire (M) du premier module de sécurité (AS), ladite mémoire (M) étant non volatile,
- on chiffre dans le premier module (AS) la clef (TA) applicative, à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme de cryptage (ALGO2), ladite clef (TA) applicative se trouvant dans ladite mémoire (M),
- on envoie au deuxième module (EI) des données (DONNEES) comprenant la clef (TA) applicative chiffrée,
- lors de chaque chargement, on calcule dans le deuxième module (EI) la clef (T1) d'exploitation à partir de l'information propre au deuxième module (EI), de la clef de transport (T) et de l'algorithme de diversification (ALGO1), ladite même clef de transport (T) se trouvant dans la mémoire (M) non volatile de chaque deuxième module (EI) de sécurité dudit ensemble (S), ladite clef (T1) d'exploitation n'étant pas enregistrée dans la mémoire (M) dudit deuxième module,

- on déchiffre dans le deuxième module (EI) la clef applicative (TA) chiffrée, à partir d'informations comprenant ladite clef (T1) d'exploitation et d'un algorithme de décryptage (ALGO2P) inverse de l'algorithme de cryptage (ALGO2).

2 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) l'information propre au deuxième module (EI), préalablement au calcul dans le premier module (AS) de la clef (T1) d'exploitation.

3 - Procédé selon les revendications 1 ou 2, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) un nombre aléatoire issu du deuxième module (EI), préalablement au chiffrement dans le premier module (AS) de la clef applicative (TA).

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au premier module (AS) une information relative à une clef applicative (TA), préalablement au chiffrement dans ledit module (AS) de la clef applicative (TA).

5 - Procédé selon la revendication 4, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On choisit la clef applicative (TA) à chiffrer à partir de ladite information.

6 - Procédé selon l'une des revendications précédentes, caractérisé en ce que chaque chiffrement d'une clef applicative (TA) destinée à un deuxième module (EI) est unique.

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que les données (DONNEES) comprenant la clef applicative (TA) chiffrée sont intègres.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On envoie au deuxième module (EI) une information relative à une clef applicative (TA), préalablement au déchiffrement dans ledit module (EI) dudit ensemble (S) de la clef applicative (TA) chiffrée.

9 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On enregistre dans le deuxième module (EI), après le déchiffrement de la clef applicative (TA) chiffrée, ladite clef (TA) dans ledit module (EI).

10 - Procédé selon la revendication 9, caractérisé en ce que l'enregistrement dans ledit deuxième module (EI) de la clef applicative (TA) se fait en fonction de l'information relative à une clef applicative (TA).

11 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- On vérifie que la clef applicative (TA) est authentique.

12 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le premier module de sécurité (AS) est une carte à puce.

13 - Procédé selon l'une des revendications précédentes, caractérisé en ce que la mémoire (M) est une mémoire réinscriptible.

14 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'un deuxième module (EI) comprend plusieurs clefs applicatives (TA).

15 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le premier module (AS) comporte plusieurs clefs applicatives (TA).

16 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- Postérieurement au chiffrement de la clef applicative (TA), on efface la clef (T1) d'exploitation sauvegardée temporairement dans une deuxième mémoire volatile du premier module (AS).

17 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- Postérieurement au déchiffrement de la clef applicative (TA), on efface la clef (T1) d'exploitation sauvegardée temporairement dans une deuxième mémoire (M2) volatile du deuxième module (EI).

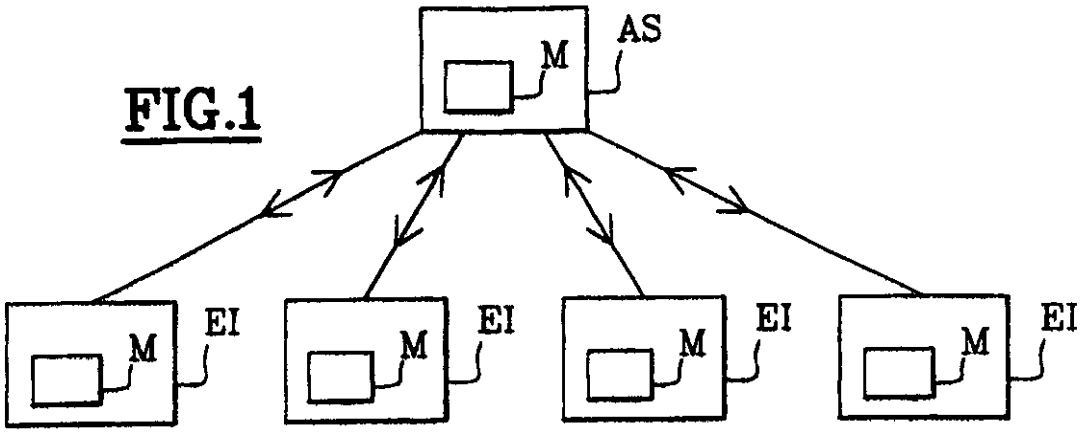
18 - Procédé selon les revendications 2 à 4 précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- L'information aléatoire, l'information relative (REF1) à une clef applicative (TA) et l'information (SN) propre au deuxième module (EI) sont envoyées au premier module (AS) au moyen d'une unique première commande (EXPORTKEY).

19 - Procédé selon les revendications 1 et 2 précédentes, caractérisé en ce qu'il comporte en outre une étape supplémentaire selon laquelle :

- La clef applicative (TA) chiffrée et l'information (REF2) relative à une clef applicative (TA), sont envoyées au deuxième module (EI) au moyen d'une unique deuxième commande (IMPORTKEY).

FIG.1



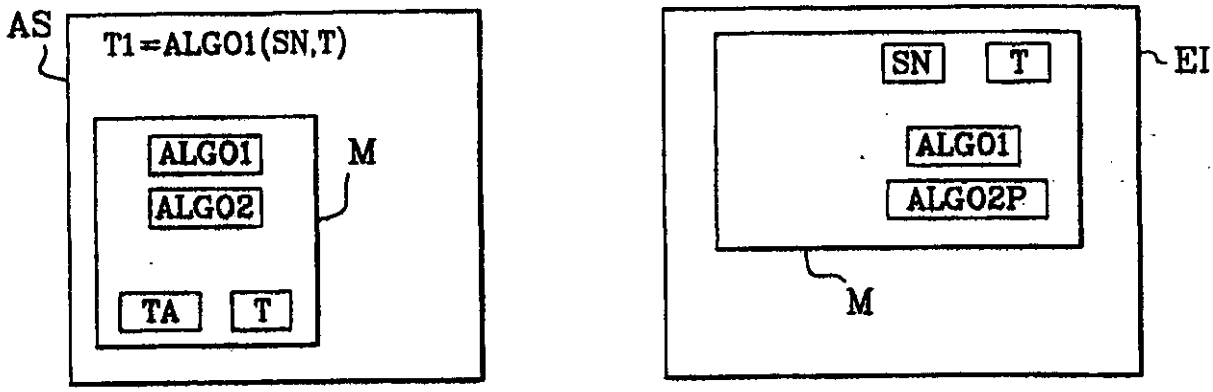


FIG.2

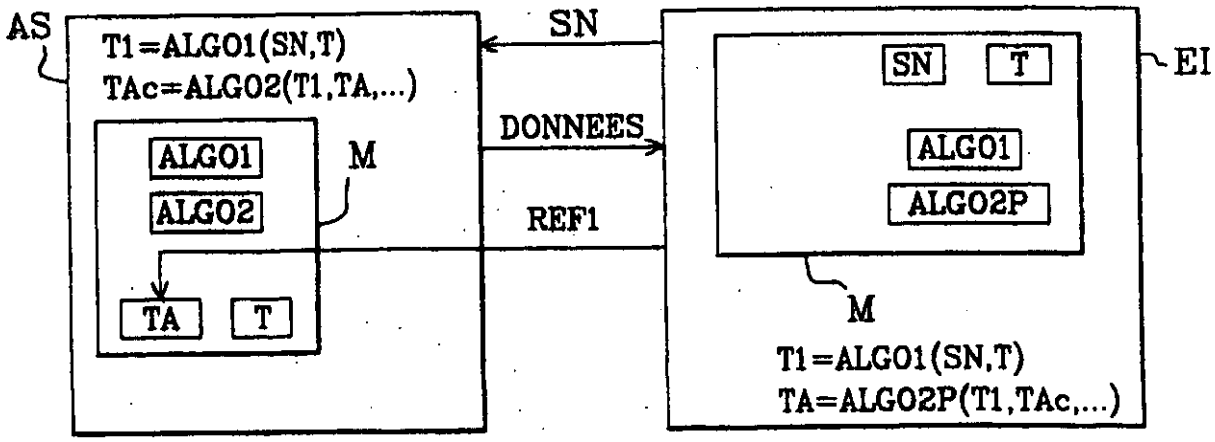


FIG.3

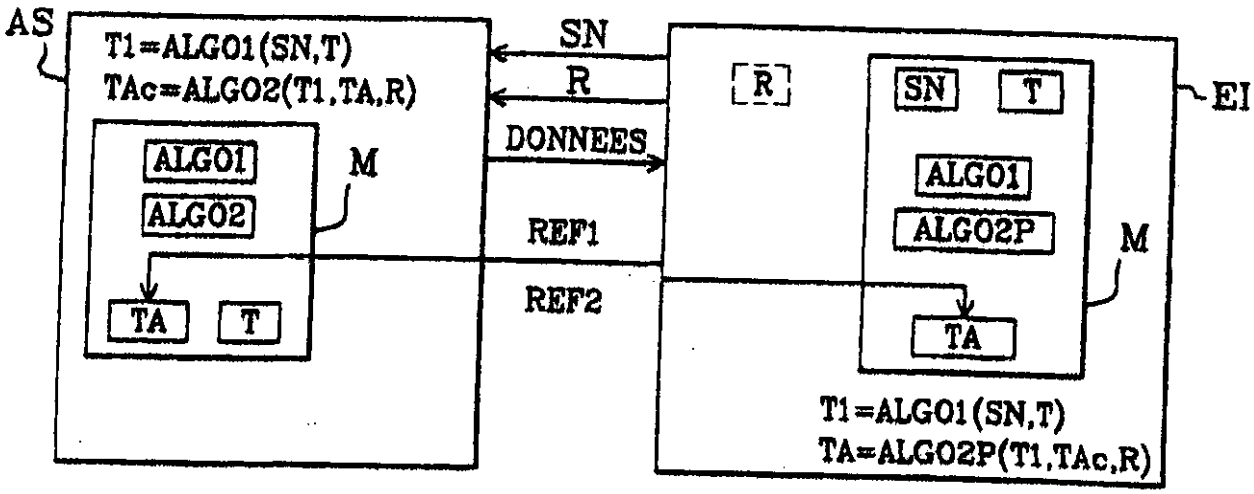

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
M
TA
T
SN
R
DONNEES
REF1
REF2
R
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.4

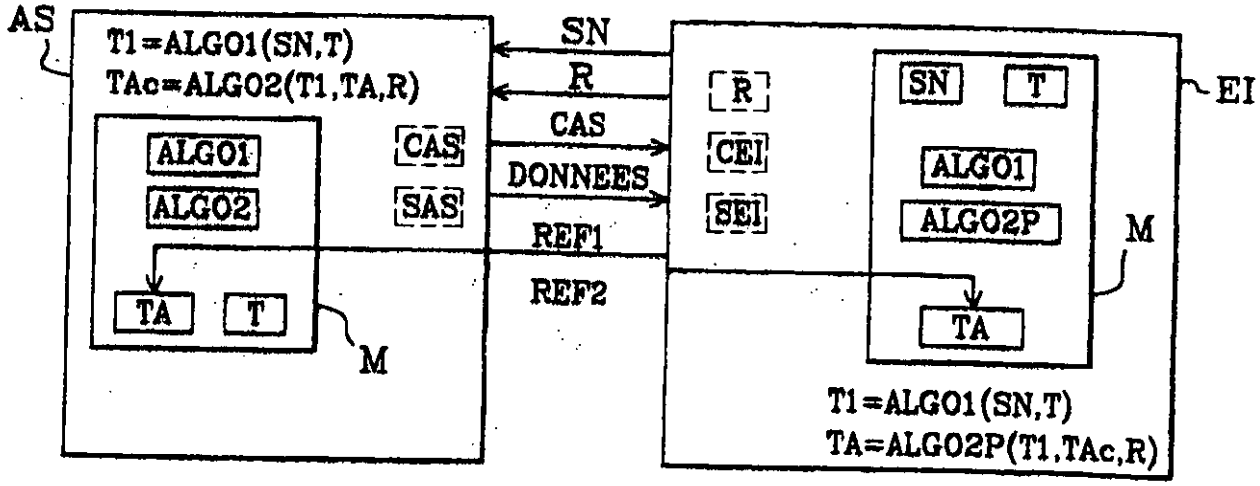

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
SN
R
CAS
DONNEES
REF1
REF2
R
CEI
SEI
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.5

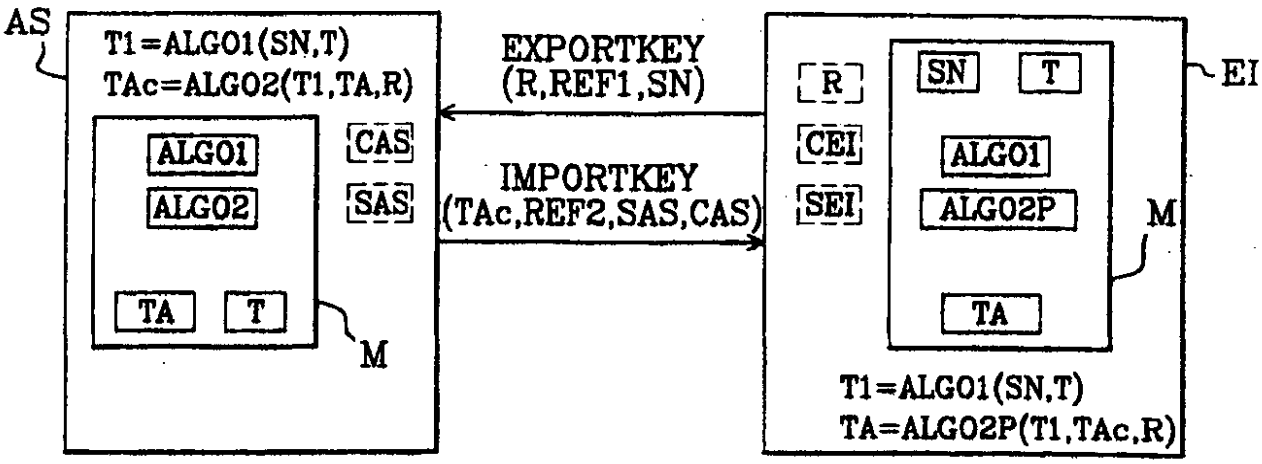

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
EXPORTKEY
(R,REF1,SN)
IMPORTKEY
(TAc,REF2,SAS,CAS)
R
CEI
SEI
SN
T
ALGO1
ALGO2P
TA
M
EI
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.6

TRAITE DE COOPERATION EN MATIERE DE BREVETS

09/889524

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
76.0546		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 00099	18/01/2000	18/01/1999
Déposant		
SCHLUMBERGER SYTEMES et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n° 5

[X] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP 00/00099

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) cité dans la demande colonne 5, ligne 55 -colonne 7, ligne 40 colonne 8, ligne 5 - ligne 10	1,3,6,9
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) abrégé	1,3,6,9
A	page 5, ligne 17 - ligne 30 page 6, ligne 27 -page 7, ligne 12 page 7, ligne 20 -page 10, ligne 18	12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 juillet 1997 (1997-07-10) abrégé page 9, ligne 13 - ligne 23	1,4,5

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents citées:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
5 avril 2000	11/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/ 00/00099

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 décembre 1997 (1997-12-11) page 6, ligne 17 - ligne 22 page 12, ligne 29 -page 14, ligne 2	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 décembre 1995 (1995-12-27) abrégé figure 1	1,7
A	EP 0 725 512 A (IBM) 7 août 1996 (1996-08-07) colonne 10, dernier alinéa -colonne 11, ligne 10; revendication 1	16,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna[illegible]al Application No
PC[illegible] 00/00099

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5517567	A	14-05-1996	NONE		
FR 2681165	A	12-03-1993	NONE		
WO 9724831	A	10-07-1997	AU	1425197 A	28-07-1997
WO 9747109	A	11-12-1997	CN	1227686 A	01-09-1999
			EP	0903026 A	24-03-1999
EP 0688929	A	27-12-1995	US	5686904 A	11-11-1997
			ZA	9505429 A	13-02-1996
EP 0725512	A	07-08-1996	US	5604801 A	18-02-1997
			JP	8340330 A	24-12-1996

Int[illegible]ional Application No
PC[illegible] 00/00099

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 517 567 A (EPSTEIN PHILIP) 14 May 1996 (1996-05-14) cited in the application column 5, line 55 -column 7, line 40 column 8, line 5 - line 10	1,3,6,9
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract	1,3,6,9
A	page 5, line 17 - line 30 page 6, line 27 -page 7, line 12 page 7, line 20 -page 10, line 18	12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 July 1997 (1997-07-10) abstract page 9, line 13 - line 23	1,4,5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 April 2000	11/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 December 1997 (1997-12-11) page 6, line 17 - line 22 page 12, line 29 -page 14, line 2	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 December 1995 (1995-12-27) abstract figure 1	1,7
A	EP 0 725 512 A (IBM) 7 August 1996 (1996-08-07) column 10, last paragraph -column 11, line 10; claim 1	16,17

INTERNATIONAL SEARCH REPORT

inf[redacted]e on patent family members

Int[redacted]ional Application No
P[redacted]R 00/00099

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5517567 A	14-05-1996	NONE	
FR 2681165 A	12-03-1993	NONE	
WO 9724831 A	10-07-1997	AU 1425197 A	28-07-1997
WO 9747109 A	11-12-1997	CN 1227686 A	01-09-1999
		EP 0903026 A	24-03-1999
EP 0688929 A	27-12-1995	US 5686904 A	11-11-1997
		ZA 9505429 A	13-02-1996
EP 0725512 A	07-08-1996	US 5604801 A	18-02-1997
		JP 8340330 A	24-12-1996

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition 20 juillet 2000 (20.07.00)	
Demande internationale no: PCT/FR00/00099	Référence du dossier du déposant ou du mandataire: 76.0546
Date du dépôt international: 18 janvier 2000 (18.01.00)	Date de priorité: 18 janvier 1999 (18.01.99)
Déposant: BUTNARU, Dan etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

10 mai 2000 (10.05.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé:

J. Zahra
no de téléphone: (41-22) 338.83.38

09/889524 Translation

09/889524

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 76.0546	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00099	International filing date (*day/month/year*) 18 January 2000 (18.01.00)	Priority date (*day/month/year*) 18 January 1999 (18.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant SCHLUMBERGER SYSTEMES		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 10 May 2000 (10.05.2000)	Date of completion of this report 09 April 2001 (09.04.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00099

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-14 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☒ the claims:

pages 1-19 . as originally filed
pages _____ . as amended (together with any statement under Article 19
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☒ the drawings:

pages 1/3-3/3 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☐ the sequence listing part of the description:

pages _____ . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

VIII. Certain observations on the international application

- the application key is decrypted in the second module **on the basis of the encrypted application key (TAc)**.

2. As regards the dependent claims, the following points are not clear:

- What is the point of sending a random number (claim 3) or information on an adaptive key (claim 4) to the first module?
- How can every encryption be unique (claim 6)?
- How can the integrity of the data (claim 7) or the authenticity of the application key (claim 11) be verified?

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-19	**YES**
	Claims		**NO**
Inventive step (IS)	Claims		**YES**
	Claims	1-19	**NO**
Industrial applicability (IA)	Claims	1-19	**YES**
	Claims		**NO**

2. Citations and explanations

Reference is made to the following documents:

D1: FR-A-2 681 165 (GEMPLUS CARD INT) 12 March 1993
D2: US-A-5 517 567 (EPSTEIN PHILIP) 14 May 1996,
cited in the application

1. The wording of independent claim 1 in its present form is so **vague and general** that, in the absence of the missing essential features (see Box VIII), it cannot be differentiated from prior art document D1, which discloses the same subject matter (secure loading of a communication key from a first module to a set of second modules) and describes the same kind of solution (both modules have identical memory portions; information is encrypted in the first module; information is decrypted in the second module; and encryption and decryption are performed on the basis of said identical memory portions) as the present application (see, in particular, figures 2 and 3 and the corresponding text in the description).

2. The same objection relating to a lack of inventive step (PCT Article 33(1) and (3)) could be raised on

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to the requirement of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in documents D1 and D2 has not been indicated in the description, nor have these documents been cited.

2. The reference signs denoting the encrypted application key (TAc) and the information specific to the second module (SN) should have been placed, between parentheses, in the claims (PCT Rule 6.2(b)).

3. To comply with the requirements of PCT Rule 5.1(a)(iii), the introductory part of the description should have been made consistent with the new claims submitted by the applicant.

   In particular, the part of the description in which the technical problems addressed and the solutions thereto are discussed (pages 1 and 2) should have been rewritten in view of the content of documents D1 and D2.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Method claim 1 does not contain all of the **essential features necessary for the definition of the invention**, contrary to the requirements of PCT Article 6 in combination with PCT Rule 6.3(b).

1a. Indeed, claim 1 does not specify that the **information specific to the second module must be sent to the first module prior to the encryption of the adaptive key in the first module.**
This feature could have been drawn from dependent claim 2.

1b. The technical features of claims 16 and 17 enhance application key loading security. They appear to match the aim of the present application, in the light of the description (page 4, lines 1-10; page 7, lines 1-4; page 8, lines 3-7), and thus appear to be essential. Said features should also have been included in claim 1.

1c. Claim 1 should also contain the following technical features:

- the application key (TA), the diversification algorithm (ALGO1) and the encryption algorithm (ALGO2) are located in the first module (AS);
- the diversification algorithm (ALGO1) and the decryption algorithm (ALGO2P) are located in the second module;
- the application key is encrypted in the first module **to give an encrypted application key (TAc);**

the basis of document D2 (see the passages cited in the international search report).

3. Dependent claims 2-19 do not appear to contain any additional features which, combined with the subject matter of claim 1, would involve an inventive step (PCT Article 33(1) and (3)). Said features are known or directly derivable from the cited documents, or are alternative embodiments that have no inventive meaning in themselves.

09/889524

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

4T

Référence du dossier du déposant ou du mandataire 76.0546	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/00099	Date du dépot international *(jour/mois/année)* 18/01/2000	Date de priorité *(jour/mois/année)* 18/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/08		
Déposant SCHLUMBERGER SYTEMES et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
10/05/2000	09.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax +49 89 2399 4465	Fonctionnaire autorisé Agreda Labrador, A

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00099

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-14 version initiale

Revendications, N°:

1-19 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n^{os} :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-19
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-19
Possibilité d'application industrielle	Oui :	Revendications	1-19
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Il est fait référence aux documents suivants:

D1: FR-A-2 681 165 (GEMPLUS CARD INT) 12 mars 1993
D2: US-A-5 517 567 (EPSTEIN PHILIP) 14 mai 1996, cité dans la demande

Concernant le point V: Déclaration motivée selon l' Article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. La formulation actuelle de la revendication indépendante 1 est si **vague et générale** que, sans les caractéristiques essentielles manquantes (voir point VIII), elle ne se différencie de l'état de la technique représenté par le document D1, celui-ci exposant le même objet (un chargement sécurisé d'une clef de communications à partir d'un premier module vers un ensemble de deuxièmes modules) et décrivant le même type de solution (tous les deux modules ont des portions de mémoire identiques; on crypte l'information dans le premier module; on décrypte l'information dans le deuxième module; le cryptage et le décryptage sont effectués à partir de ces portions de mémoire identiques) que la présente demande (voir en particulier les figures 2 et 3 et le texte correspondant dans la description).

2. La même objection de manque d'activité inventive (Articles 33(1) et (3) PCT) pourrait être soulevée en partant du document D2 (voir passages cités dans le Rapport de Recherche Internationale).

3. Les revendications dépendantes 2-19 ne semblent pas contenir de caractéristiques supplémentaires qui, en combinaison avec l'objet de la revendication 1, impliqueraient une activité inventive (Articles 33(1) et (3) PCT). Celles-ci sont connues soit directement dérivables des documents cités ou soit des variantes de réalisation sans signification inventive propre.

Concernant le point VII: Irrégularités dans la demande internationale

1. Contrairement à ce qu'exige la Règle 5.1(a)(ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1 et D2 et ne cite pas ces documents.

2. Les signes de référence correspondant à la clef applicative chiffrée (TAc) et à l'information propre au deuxième module (SN) auraient dû être introduits, entre parenthèses, dans les revendications (Règle 6.2(b) PCT).

3. En vue de remplir les conditions énoncées à la Règle 5.1(a)(iii) PCT, la partie introductive de la description aurait dû être mise en conformité avec les nouvelles revendications proposées par le Demandeur.

   En particulier, la partie de la description exposant les problèmes techniques traités et la solution apportée à ces problèmes (pages 1-2) aurait dû être révisée, eu égard au contenu des documents D1 et D2.

Concernant le point VIII: Observations relatives à la demande internationale

1. La revendication de procédé 1 ne contient pas toutes les **caractéristiques essentielles nécessaires à la définition de l'invention**, conformément à l'Article 6 PCT pris en combinaison avec la Règle 6.3(b) PCT:

1a. En effet la revendication 1 ne précise pas que **l'information propre au deuxième module doit être envoyée au premier module, préalablement au chiffrement dans le premier module de la clef adaptative**.
Cette caractéristique aurait pû être tirée de la revendication dépendante 2.

1b. Les caractéristiques techniques des revendications 16 et 17 permettent d'améliorer la sécurité du chargement d'une clef applicative. Elles semblent correspondre avec le but de la présente demande, compte tenu de la description (page 4, lignes 1-10; page 7, lignes 1-4; page 8, lignes 3-7) et semblent donc

essentielles. Ces caractéristiques auraient dû également être incluses dans la revendication 1.

1c. La revendication 1 devrait contenir par ailleurs les caractéristiques techniques suivantes:

- La clef applicative (TA), l'algorithme de diversification (ALGO1) et l'algorithme de cryptage (ALGO2) se trouvent dans le premier module (AS);
- L'algorithme de diversification (ALGO1) et l'algorithme de décryptage (ALGO2P) se trouvent dans le deuxième module;
- On chiffre dans le premier module la clef applicative, **obtenant une clef applicative chiffrée (TAc)**;
- On déchiffre dans le deuxième module la clef applicative **à partir de la clef applicative chiffrée (TAc)**.

2. Concernant les revendications dépendantes, il n'est pas clair:

- à quoi sert d'envoyer au premier module un nombre aléatoire (rev. 3) ou une information relative à une clef adaptative (rev. 4);
- comment chaque chiffrement peut être unique (rev. 6);
- comment l'on vérifie que les données sont intègres (rev. 7) ou que la clef applicative est authentique (rev. 11).

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 570510
FR 9900462

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) * colonne 5, ligne 55 - colonne 7, ligne 40 * * colonne 8, ligne 5 - ligne 10 *	1,3,6,9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) * page 5, ligne 17 - ligne 30 * * page 7, ligne 20 - page 10, ligne 18 *	1-3,6,9, 12
A	WO 97 24831 A (MCI COMMUNICATIONS CORP) 10 juillet 1997 (1997-07-10) * abrégé * * page 9, ligne 13 - ligne 23 *	1,4,5
A	WO 97 47109 A (SIEMENS AG ;EUCHNER MARTIN (DE); KESSLER VOLKER (DE)) 11 décembre 1997 (1997-12-11) * page 6, ligne 17 - ligne 22 * * page 12, ligne 29 - page 14, ligne 2 *	7,11
A	EP 0 688 929 A (NANOTEQ PTY LTD) 27 décembre 1995 (1995-12-27) * abrégé * * figure 1 *	1,7

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L

Date d'achèvement de la recherche: 11 octobre 1999

Examinateur: Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)